ABSTRACT

A network intrusion detection unit (NIDU) identifies a protocol used to transmit a packet and the flow to which the packet belongs. The NIDU determines whether a rules table exists for the protocol, and determines, if the rules table exists, whether a state table includes a matching flow entry corresponding to the flow. If the state table includes the matching flow entry, the NIDU determines whether a state of the flow will transition from a current state indicated in the matching flow entry to a valid destination state indicated in a state-transition rule in the rules table. If the state of the flow will not transition to a valid destination state, the NIDU discards the packet.